METHOD FOR BROADCAST ENCRYPTION AND KEY REVOCATION OF STATELESS RECEIVERS

ABSTRACT OF THE DISCLOSURE

A tree is used to partition stateless receivers in a broadcast content encryption system into subsets. Two different methods of partitioning are disclosed. When a set of revoked receivers is identified, the revoked receivers define a relatively small cover of the non-revoked receivers by disjoint subsets. Subset keys associated with the subsets are then used to encrypt a session key that in turn is used to encrypt the broadcast content. Only non-revoked receivers can decrypt the session key and, hence, the content.